

IN THE CLAIMS

Please amend the claims as follows:

Claim 1 (Currently Amended): A communication processing apparatus for executing a communication process via a network, ~~characterized in that~~ comprising:

a communication unit configured to implement a communication process related to an authentication process according to a predetermined authentication method, the communication process being [[is]] performed in order to acquire secret information permitted to be disclosed only to devices in a local network corresponding to said authentication method; unique identification information of a communication destination device in said communication process is acquired by data processing at a network layer or lower of an OSI reference model; unique identification information of an authentication partner device is acquired in an authentication sequence of said authentication method as data processing at an application layer of the OSI reference model; said acquired unique identification information of said communication destination device is ~~matched~~ compared with said acquired unique identification information of said authentication partner device; and ~~in accordance with a passed or failed state of the matching~~ based upon a successful match resulting from the compared data, a process is executed to judge whether said authentication partner device is a device connected to a same local network as a local network to which a local device being a communication source device is connected.

Claim 2 (Currently Amended): The communication processing apparatus as claimed in Claim 1, ~~characterized that~~ wherein at least one of said unique identification information received from said authentication partner device is received as processed data generated by an encryption process or a hash value generation process based on secret information shared with said communication source device.

Claim 3 (Currently Amended): The communication processing apparatus as claimed in Claim 1, ~~characterized in that~~ wherein identification information received from said communication destination device is a node unique ID defined in IEEE 1394 standards.

Claim 4 (Currently Amended): The communication processing apparatus as claimed in Claim 1, ~~characterized in that~~ wherein said communication processing apparatus is configured to receive, as identification information received from said communication destination device, identification information acquired from a PHY communication unit of said communication destination device and identification information acquired by a network communication unit of said communication destination device, and ~~match~~ compare a plurality of these identification information.

Claim 5 (Currently Amended): The communication processing apparatus as claimed in Claim 1, ~~characterized in that~~ wherein identification information received from said communication destination device is a device address defined in communication standards.

Claim 6 (Currently Amended): The communication processing apparatus as claimed in Claim 1, ~~characterized that~~ wherein said communication processing apparatus is configured to receive, as identification information received from said communication destination device, a device address as a source address of a packet transmitted from said communication destination device, and a device address stored in a packet by data processing at an application ~~[[level]]~~ layer or data based on the device address at the application ~~[[level]]~~ layer, and ~~[[match]]~~ compare a plurality of these device addresses.

Claim 7 (Currently Amended): A communication controlling method for executing a communication process via a network, said method ~~characterized by~~ comprising:

~~an identification information acquiring step of~~ acquiring unique identification information of a communication destination device in a communication process by data processing at a network layer or lower of an OSI reference model, and acquiring unique identification information of an authentication partner device in an authentication sequence of a predetermined authentication method as data processing at an application layer of the OSI reference model;

~~a matching processing step of~~ performing a matching of said acquired unique identification information of said communication destination device with said acquired unique identification information of said authentication partner device; and

judging, ~~in accordance with a passed or failed state of the matching based upon a successful match resulting from the compared data identifying~~, whether said authentication partner device is a device connected to a same local network as a local network to which a local device being a communication source device is connected.

Claim 8 (Currently Amended): The communication controlling method as claimed in Claim 7, ~~characterized in that~~ wherein in said ~~identification information~~ acquiring step, at least one of said unique identification information received from said authentication partner device is received as processed data generated by an encryption process or a hash value generation process based on secret information shared with said communication source device.

Claim 9 (Currently Amended): The communication controlling method as claimed in Claim 7, ~~characterized in that~~ wherein identification information received from said communication destination device is a node unique ID defined in IEEE 1394 standards.

Claim 10 (Currently Amended): The communication controlling method as claimed in Claim 7, ~~characterized in that~~ wherein in said ~~identification information~~ acquiring ~~step is a step of receiving~~ receives, as identification information received from said communication destination device, identification information acquired from a PHY communication unit of said communication destination device and identification information acquired by a network communication unit of said communication destination device, and said ~~matching~~ comparing processing ~~[[step]]~~ matches a plurality of these identification information.

Claim 11 (Currently Amended): The communication controlling method as claimed in Claim 7, ~~characterized in that~~ wherein identification information received from said communication destination device is a device address defined in communication standards.

Claim 12 (Currently Amended): The communication controlling method as claimed in Claim 7, ~~characterized in that:~~ wherein said ~~identification information~~ acquiring ~~[[step]]~~ receives, as identification information received from said communication destination device, a device address as a source address of a packet transmitted from the communication destination device, and a device address stored in a packet by data processing at the application ~~[[level]]~~ layer or data based on the device address at the application ~~[[level]]~~ layer, and

said matching ~~processing step~~ matches a plurality of these device addresses.

Claim 13 (Currently Amended): A computer ~~program for executing a readable~~
storage medium encoded with computer program instructions which, when executed, cause a
processor to execute a method of communication ~~process~~ via a network, said ~~program~~
~~characterized by method~~ comprising:

~~an identification information acquiring step of~~ acquiring unique identification
information of a communication destination device in a communication process by data
processing at a network layer or lower of an OSI reference model, and acquiring unique
identification information of an authentication partner device in an authentication sequence of
a predetermined authentication method as data processing at an application layer of the OSI
reference model;

~~a matching processing step of~~ performing a matching of said acquired unique
identification information ~~identification information~~ of said communication destination
device with said acquired unique identification information of said authentication partner
device; and

~~a judging step of~~ judging, based upon a successful match resulting from the compared
data identifying in accordance with a passed or failed state of said matching, whether said
authentication partner device is a device connected to a same local network as a local
network to which a local device being a communication source device is connected.